

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

IN THE MATTER OF THE SEARCH OF) Case No. 3:18-mj-00489-DMS
)
Samsung cellphone S/N: R38JAQADNJV) **UNDER SEAL**
located in GMC Yukon JLV948; Acer)
laptop S/N:)
NXGHJAA0028130D3E77600; My)
Passport hard drive with thumb drive;)
Silver cell phone located on Parke's)
person; Samsung tablet S/N:
R52JB17QP0B; Samsung cell phone
Galaxy S7; Samsung cell phone IMEI:
355077081992876; Black and orange
E+L phone; Black iPhone located on
Hansen's person

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, WENDY M. TERRY, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a Samsung cellphone S/N: R38JAQADNJV located in GMC Yukon JLV948; Acer laptop S/N: NXGHJAA0028130D3E77600; My Passport hard drive with thumb drive; Silver cell phone located on Parke's person; Samsung tablet S/N: R52JB17QP0B; Samsung cell phone Galaxy S7; Samsung cell phone IMEI: 355077081992876; Black and orange E+L phone; Black iPhone located on Hansen's person (hereinafter "SUBJECT

DEVICE”), as described in Attachment A, for the things described in Attachment B. The United States requests authority to seize from the SUBJECT DEVICE the items described in Attachment B, which your Affiant submits constitute instrumentalities and evidence of violations of 21 U.S.C. 846, Conspiracy to distribute 500 grams or more of methamphetamine and 21 U.S.C. 841(a)(1) and (b)(1)(A), Possession with the intent to distribute controlled substances.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been since June 2014. I am currently assigned to the Violent Crime Squad in the FBI Anchorage Field Office. During my time with the FBI, I have lead and participated in investigations involving violent crimes, threats, robbery, drugs, and child pornography. I have also been an affiant on multiple federal search warrants seeking information relating to investigations of threats, robbery, drugs, and child pornography offenses. Prior to June 2014 I was employed with the Savannah Chatham Metropolitan Police Department (SCMPD) in Savannah, Georgia, as a Police Officer and Detective. As a Police Officer and Detective, I was assigned to the Patrol Unit, Crime Suppression Unit, Property Crimes Detective Unit, and Homicide Detective Unit. During these assignments I led and participated in a large number of property crime investigations; led and participated in a large number of drug-related arrests, including buy-bust operations, reverse buy operations, and surveillance operations; and assisted in the preparation and execution of numerous search warrants and arrest warrants. The

Affidavit in Support of Search Warrant 2

execution of these search and arrest warrants led to the seizure of firearms, ammunition, magazines, controlled substances, packing implements, United States currency, vehicles, communication devices, computers, receipts, ledger books, and other documents relating to the transportation, ordering, purchase and distribution of controlled substances, and recovery of stolen property.

3. This affidavit is made in support of an application for a warrant to search a Samsung cellphone S/N: R38JAQADNJV located in GMC Yukon JLV948; Acer laptop S/N: NXGHJAA0028130D3E77600; My Passport hard drive with thumb drive; Silver cell phone located on Parke's person; Samsung tablet S/N: R52JB17QP0B; Samsung cell phone Galaxy S7; Samsung cell phone IMEI: 355077081992876; Black and orange E+L phone; Black iPhone located on Hansen's person (hereinafter "SUBJECT DEVICE"), more particularly described in Attachment A, for the items specified in Attachment B, and to seize the items specified in Attachment B. As a result of the investigation described below, I submit that there is probable cause to believe that evidence of violations of 21 U.S.C. 846, Conspiracy to distribute 500 grams or more of methamphetamine (hereinafter "SUBJECT OFFENSE"), may be present on the SUBJECT DEVICE.

4. I am familiar with the information contained in this affidavit based upon the investigation I have conducted along with other federal, state, and local law enforcement officials. This investigation has included numerous meetings and the sharing of information with law enforcement officers and law enforcement

Affidavit in Support of Search Warrant 3

personnel, interviews of witnesses and other persons with information, the review of interviews conducted by other law enforcement officers of witnesses and other persons with information, the review of other relevant reports, the execution of search warrants and database searches. Based on this investigation, I submit that there is probable cause to believe that there is evidence on the SUBJECT DEVICE of the commission of the SUBJECT OFFENSE.

5. Because I submit this affidavit for the limited purpose of securing a search warrant, I have not included each and every fact known to me or the government regarding the investigation described herein. Instead, I have only included those facts necessary to establish that there is probable cause to believe that instrumentalities and evidence of violations of the SUBJECT OFFENSE may be located on the SUBJECT DEVICE.

RELEVANT STATUTES AND REGULATIONS

6. The relevant statutory authority and terms used in this affidavit and its attachments are described and defined below.

7. This search warrant seeks instrumentalities, contraband, and evidence of violations of the following:

- a. Title 21, United States Code, Section 841(a), which states: "It shall be unlawful for any person knowingly or intentionally (1) to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance; or (2) to create,
- Affidavit in Support of Search Warrant 4

distribute, or dispense, or possess with intent to distribute or dispense, a counterfeit substance.

- b. Title 21, United States Code, Section 846, which states: “Any person who attempts or conspires to commit any offense defined in this subchapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

8. The following technical terms are relevant to my affidavit in support of this application for a search warrant.

- a. *Digital device*: A “digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including central processing units; desktop, laptop or notebook computers; tablets, internet-capable cellular phones (smart phones), or personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, flash drives, thumb drives, floppy

disks, compact disks, DVDs, magnetic tapes, and memory chips; and security devices.

b. Image or copy: An “image or copy” is an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.

c. The terms “*records*” and “*information*” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writings, drawings or paintings); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

FACTS SUPPORTING PROBABLE CAUSE

Background of the Investigation

9. On 7/26/2018, agents and officers with the Joint Task Force Airport Interdiction Team were notified by the Whittier Police Department that the agents of the Alaska Marine Highway terminal in Whittier Alaska reported a suspicious

Affidavit in Support of Search Warrant 6

passenger who disembarked from the M/V Kennicott, which had arrived from Bellingham, Washington after stopping in several Southeast Alaska communities. The male, who was later identified as Eric Hansen, was seen getting into the passenger seat of a silver/grey GMC Yukon bearing Alaska license plate JLV948.

10. Whittier Police Department conducted a traffic stop on the vehicle. Marshal Parke was driving the vehicle, and Eric Hansen was in the passenger seat.

Another woman was in the backseat. A scent-detection canine performed a sniff of the exterior of the Yukon "indicating" to the odor of controlled substances emanating from the vehicle.

11. A search warrant was applied for and granted by the State of Alaska. Agents and officers with the airport interdiction team executed the search of the vehicle. The search yielded approximately 33 pounds of methamphetamine, which were located in a backpack that Hansen had been seen wearing at the ferry terminal. There was approximately \$8,000 cash US currency located in a black leather brief in the back of the vehicle. The briefcase that contained a boarding pass for Marshal Parke, a scale with drug residue on it, other items of drug paraphernalia (glass pipe with burnt edges). A small bag of white powdered substance was found in between the driver seat where Marshal Parke was driving and the center console. The boarding pass was dated for 7/20/2018, departing Seattle Washington and returning to Anchorage Alaska. Eric Hansen's travel records showed Hansen boarded the M/V Kennicott in Bellingham, Washington on 7/21/2018. Also, found in the vehicle was a

Affidavit in Support of Search Warrant 7

Western Union money transfer dated for 7/17/2018 the sender was Tammy Barclay from Anchor Point sending \$600 USD to Marshal Parke in Washington. A hotel receipt at the EconoLodge, located in Fife Washington, dated for 7/18-19/2018 with Parke's name on it was found in the vehicle. Agents seized a cell phone from each occupant of the vehicle and several more electronic devices (laptop and tablet),
10/3/18
for u.T.
and the My Passport w/ thumb drive

12. In my training and experience, and in speaking to other investigators, this amount of methamphetamine has an approximate wholesale value of \$225,000, and a street value far exceeding that for sales of user quantities. It is also in my training and experience that drug dealers who travel between states use their phones to facilitate their crime.
10/2/18
for u.T.

All of the devices and cellphones listed in items to be searched were found either in the vehicle or on the owner (occupant of vehicle).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described below in Attachment B, this warrant seeks authority to search the content of the SUBJECT DEVICES capable of holding the items described in Attachment B. The searching of the SUBJECT DEVICES is appropriate for several reasons. First, the search of electronic devices may allow law enforcement to identify any other associates or accomplices in the distribution of drugs. Second, in my training and experience, I know that individuals involved in joint criminal activity frequently communicate with one another through cell phones, instant messaging, and other social media platforms. These communications may address planning and execution of the crime, as well as attempts to evade law enforcement.

Affidavit in Support of Search Warrant 8

Third, I am familiar with instances in which individuals involved in criminal activity have spoken to others through direct communications and other forms of communications, to include text messaging, instant messaging, and social media platforms, about their crimes attributes of digital evidence.

14. Searches and seizures of evidence from computers and other Internet access devices require agents to seize most or all electronic items (hardware, software, passwords and instructions) to be processed later by appropriate personnel in a controlled environment.

15. Searching digital evidence systems for criminal evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even “hidden,” erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

16. Computers and other digital communications devices contain volatile memory that contains information only while the device is in a powered on and/or running state. I know that powering off the device may result in the loss of the volatile information. Adding an external evidence storage device will cause minor changes to the state of the computer but will allow for the best effort in fully capturing the state of the running evidence. This capture of information requires technical

Affidavit in Support of Search Warrant 9

expertise to ensure the resulting data can be examined by all subsequent investigators. This captured information may include current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details relevant to use of the system.

17. Law enforcement personnel trained in searching and seizing computer data will seize items of evidentiary value, and transport the same to an appropriate law enforcement laboratory for off-site review. The electronic media will be reviewed for the evidence described in Attachment B in accordance with and as defined by the review protocols described below.

18. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long

Affidavit in Support of Search Warrant 10

periods of time before they are overwritten. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. The search for these files and file fragments can take considerable time, depending on the computer user's practices.

19. I know from training and experience that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device, ownership and use of any external devices that had been attached to the computer or other digital devices, as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

SPECIFIC METHODS OF SEARCHING FOR DIGITAL EVIDENCE

20. I am seeking authority to search for, among other things, items containing digital data, more particularly described in Attachment B. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the

media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

21. The search of a computer hard drive, cell phone, or other computer storage medium is a time-consuming manual process often requiring months of work. This is so for a number of reasons, including the complexity of computer systems, the multiple devices upon which computing can take place, and the tremendous storage capacity of modern day computers, and the use of encryption or wiping software. I know from my training and experience, and from my discussions with trained computer forensic examiners, that a review of such quantities of evidence can take a significant amount of time. Second, there is a limited pool of personnel capable of conducting a forensic examination. Third, in some instances an individual may utilize encryption software or other publically-available techniques such as wiping software to hide their activities. Forensic tools are available to circumvent some of these techniques; however, these tools may require a significant allocation of resources and a substantial period of time. With rare exception, searches will not be performed on original digital evidence. Instead, I know that the first priority of a digital evidence forensic examination is the preservation of all data seized. As such, original digital media will be, wherever possible, copied, or "imaged," prior to the

start of any search for evidence. The copy will be authenticated digitally as described in the paragraph below.

22. I know that a digital forensic image is the best possible copy that can be obtained for a piece of digital media. Forensic imaging tools make an exact copy of every accessible piece of data on the original digital media. In general, the data contained on the original media is run through a hashing algorithm as described above, and a hash value for the entire device is generated. Upon completion of the imaging process, the same hash algorithm is run on the imaged copy to insure the copy is an exact duplicate of the original.

23. In the event that a piece of digital media is found not to be (a) an instrumentality of the offense, (b) a fruit of the criminal activity, (c) contraband, or (d) evidence of the offenses specified herein, it will be returned as quickly as possible.

CONCLUSION

24. Based upon the information above, your affiant submits that there is probable cause to believe that violations of Title 21 U.S.C. 846, Conspiracy to distribute 500 grams or more of methamphetamine, that the items described in Attachment B are evidence and instrumentalities of the above-described violation, and that the items described in Attachment B are likely to be found in the SUBJECT DEVICE described in Attachment A.

25. I submit that this affidavit demonstrates and establishes that there is probable cause for a warrant to search the SUBJECT DEVICE described in Attachment A, and the seizure of the items described in Attachment B. I request that the Court issue a warrant authorizing a search of the SUBJECT DEVICE is described in Attachment A, for the items described in Attachment B.

Signature Redacted

WENDY TERRY
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 3rd day of October 2018

/s/ SCOTT A. ORAVEC
U.S. MAGISTRATE JUDGE
SIGNATURE REDACTED

Scott A. Oravec
United States Magistrate Judge
District of Alaska
Anchorage, Alaska

